THE CAPCO INSTITUTE
JOURNAL
OF FINANCIAL TRANSFORMATION

OPERATIONS

Operational resilience and stress testing: Hit or myth?

GIANLUCA PESCAROLI
CHRIS NEEDHAM-BENNETT

20
YEAR ANNIVERSARY

OPERATIONAL RESILIENCE

#53 MAY 2021

THE CAPCO INSTITUTE

JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

CONTENTS

OPERATIONS

TECHNOLOGY

MILITARY

DEAR READER,

Welcome to this landmark 20th anniversary edition of the Capco Institute Journal of Financial Transformation.

Launched in 2001, the Journal has followed and supported the transformative journey of the financial services industry over the first 20 years of this millennium – years that have seen significant and progressive shifts in the global economy, ecosystem, consumer behavior and society as a whole.

True to its mission of advancing the field of applied finance, the Journal has featured papers from over 25 Nobel Laureates and over 500 senior financial executives, regulators and distinguished academics, providing insight and thought leadership around a wealth of topics affecting financial services organizations.

I am hugely proud to celebrate this 20th anniversary with the 53rd edition of this Journal, focused on 'Operational Resilience'.

There has never been a more relevant time to focus on the theme of resilience which has become an organizational and regulatory priority. No organization has been left untouched by the events of the past couple of years including the global pandemic. We have seen that operational resilience needs to consider issues far beyond traditional business continuity planning and disaster recovery.

Also, the increasing pace of digitalization, the complexity and interconnectedness of the financial services industry, and the sophistication of cybercrime have made operational disruption more likely and the potential consequences more severe.

The papers in this edition highlight the importance of this topic and include lessons from the military, as well as technology perspectives. As ever, you can expect the highest caliber of research and practical guidance from our distinguished contributors. I hope that these contributions will catalyze your own thinking around how to build the resilience needed to operate in these challenging and disruptive times.

Thank you to all our contributors, in this edition and over the past 20 years, and thank you, our readership, for your continued support!

Lance Levy, **Capco CEO**

OPERATIONAL RESILIENCE AND STRESS TESTING: HIT OR MYTH?

GIANLUCA PESCAROLI | Lecturer in Business Continuity and Organisational Resilience, and Director of the MSc in Risk, Disaster and Resilience, University College London

CHRIS NEEDHAM-BENNETT | Managing Director, Needhams 1834 Ltd.

ABSTRACT

The complexities of interconnected global risk and the growing uncertainties associated with emerging threats, such as the cascading effects of COVID-19, have challenged the existing approaches to business continuity management. Organizations are now implementing and maintaining "operational resilience". However, operational resilience is distinguished by a lack of clarity as to how this concept can be translated into validated practices and the essential elements of such practices are sometimes obscured rather than clarified by its aggressive marketing to the practitioners. This paper develops a short perspective on what the strength and weaknesses of the current approaches to operational resilience are. We believe that while operational resilience as a concept is suitable for both professionals and scholars, it should be used with caution. We further suggest that its optimal application could be in combination with stress testing scenarios, which could be applied for defining common points of failures between distinct threats, to increase the flexibility of adaptation to complex crises. We propose five practical steps for bridging theories on cascading effects and systemic risk into mature practices for "thinking the unthinkable".

1. INTRODUCTION

History may remember 2020 and 2021 as a curious interlude when platforms such as Zoom, Teams, Skype, and Google Meet became essential for human interaction. The interdependencies between organizations, society, and technology were catapulted into sharp focus during the COVID-19 pandemic. It has become clearer that any form of commerce, let alone emergency response and recovery, has been enabled or limited by the reliability of infrastructures, which are in turn dependent on energy supply and telecommunications networks. Notwithstanding the current novel situation, the complexity of networked services is nothing new. Authors, such as Linkov et al. (2014), have for years been calling for a radical shift from risk management to resilience management and adopting a system perspective. International documents and guidance published over the past decade have made some effort to promote a fresh approach in research and practice. For example, in 2015, the U.N. member states adopted the Sendai Framework for Disaster Risk Reduction (SFDRR), in which Priority 3 focuses on "investing in disaster risk reduction for resilience". Following this milestone, some new initiatives were launched, including the U.N. Private Sector Alliance for Disaster Resilient Societies (ARISE) or the "Making cities resilient 2030" campaign. The International Risk Governance Council published the "Resource guide on resilience" in 2016 and 2018 to "supplement and an alternative to conventional risk management" for situation of high uncertainties.[1]

Despite the advances outlined above, the domain of "operational resilience" remains very fragmented and the concept has both potential as well as limitations and shortfalls. Nevertheless, this is a common start point for almost all ideas that have influenced subsequent practice. However, in such a state of flux it can be difficult to separate worthwhile ideas

[1] https://bit.ly/2OxqTOK

from hyperbole. In 1974, the astronomer Carl Sagan observed that "The well-meaning contention that all ideas have equal merit seems to me to be little different from the disastrous contention that no ideas have any merit" [Sagan (1974)].

He prefaced this remark using the lovely 19th century term "paradoxers" to describe those "who invent elaborate and undemonstrated explanations." The commercial literature on operational resilience often appears to be derived from marketeers playing Scrabble; it is awash with grandiloquent claims for corporate panaceas, easy to administer systems, and even improved profitability. Consequently, the simple intent of this article is to (without "paradoxing") offer the reader some of the evidence for the judicious application of operational resilience, to discuss the genuine difficulties of doing this, and highlight the potential benefits.

2. BUSINESS CONTINUITY TO OPERATIONAL RESILIENCE, A SMALL STEP OR A "GIANT LEAP"?

The semantic schisms that had evolved through the overdifferentiation of crisis management, emergency responses, business continuity, disaster recovery, and disaster management [Smith and Elliott (2006)] have to some extent been overtaken by the use of the umbrella term "resilience". Some reviews of the academic literature, such as the one by Linnenluecke (2017), have already explained the differences and similarities between research streams in this field, including the tendency to reveal few empirical insights. However, the dangers of a rush to embrace the broad church of "resilience" was highlighted Alexander (2013). His definitive and comprehensive etymological analysis of the word "resilience" also cited others who were suspicious that, "resilience is being used as little more than a fashionable buzz-word ... there is bound to be a sense of disillusionment if the term is pushed to represent more than it can deliver. The problem lies in attempts to make resilience a full-scale paradigm or even a science."

As much of the "resilience debate" has been more semantic than pragmatic and, as Boin (2006) disarmingly noted, "Academics rarely agree on key terms," we would prefer not to add more definitions of resilience and it is hoped that the definitions of "resilience" that have been reported in the two most common standards of business continuity can provide a suitable benchmarking for the purpose of this paper. Resilience can be considered as "the ability of an organization to absorb and adapt in a changing environment [ISO (2017)], or as the "ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions" [NFPA (2019]. It should be noted that there are some differences with the standard U.N. terminology used in disaster risk reduction, which gives more emphasis to the interactions between system community and society.[2]

A specific definition for the financial services sector comes from the Basel Committee on Banking Supervision consultative document "Principles for operational resilience", issued for comment on November 6th, 2020. Section IV considers "operational resilience" as: "the ability of a bank to deliver critical operations through disruption. This ability enables a bank to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimize their impact on the delivery of critical operations through disruption. In considering its operational resilience, a bank should take into account its overall risk appetite, risk capacity, and risk profile."[3]

One could make an academic case that this is neither a giant leap nor a "paradigm shift" away from the definition of business continuity provided by ISO (2019), which describes it as the: "capability of an organization to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption." Or the common definition offered for enterprise risk management: "Enterprise risk management (ERM) is a plan-based business strategy that aims to identify, assess, and prepare for any dangers, hazards, and other potentials for disaster – both physical and figurative – that may interfere with an organization's operations and objectives."[4]

The point seems to be that operational resilience evidently demands a broader, more comprehensive approach than mere "business continuity". As argued by Herbane (2016), at the broader level, both business continuity and risk management have roles in developing resilience, but they are not its equivalent. This is particularly important when the complexities of financial transactions are considered. A technical note for State Treasuries by the International Monetary Fund specifies that "resilience comes from tackling the likelihood as well as the consequences of disruptive events" [Storkey (2011)]. More specifically, in this guidance, it is suggested that treasuries develop strategies for improving resilience after having

[2] https://bit.ly/3qr2urA
[3] https://bit.ly/3sZf6b4
[4] https://bit.ly/2Oa3AdW

completed the "business impact analysis". The idea of a comprehensive approach was alluded to by Alexander (2013) when he referenced bioecological theory, in which he states that, "resilience arises from interaction across multiple levels of functioning." He suggests that the "but" in the argument is that "it does appear that the lack of resilience at one level… can undermine resilience at other levels…" This notion of a broader remit, together with the interdependencies mentioned, militates for a panarchical approach to resilience. This "panarchy"[5] is simply a term for "a form of governance that would encompass all others" [de Puydt (1860)]. In this case, we are referring only to the need for a complex governance approach rather than adopting the notion entirely in terms of social sciences [Allen et al. (2014)].

It seems, therefore, that operational resilience appears to be the natural inheritor, or evolutionary consequence of business continuity. The main differentiator, or giant leap, is its scope, with a consequent need for panarchical or systemic management. The extant question is, is it worth it?

3. IS IT WORTH IT?

To determine its value, we need to address three very simple specific questions to evaluate the costs and benefits of the effort needed:

1. Is the global environment getting more dangerous?
2. Does resilience "work" and is it worth it?
3. What can we do to achieve it?

3.1 The global environment

The global environment is arguably more benign than it was. The aetiological paradox is that, despite or because of our preoccupation with risk, life expectancy is increasing globally; taking into account some geographic inequality it has roughly doubled since 1900 [Roser et al. (2013)]. However, simultaneously, risk is becoming more complex, interconnected, and harder to predict [Helbing (2013)]. Modern operations face increased uncertainties caused by the networked vulnerabilities of services, components, and functions [Linkov et al. (2014)]. Doubtless most organizations could have dealt with the consequences of having personnel stranded on the other side of the world during the 2010 eruption of the Icelandic volcano Eyjafjallajökull, worked through supply chain disruptions during the 2011 triple event in Japan, coped during the early stages of the COVID-19 pandemic, or endured technology failures as a consequence of weather events such as the 2021 blackout in Texas. It is debatable, however, if those same organizations could cope as easily with a concatenation of incidents, or concurrent events with cascading effects of failures impacting multiple business sectors [Pescaroli and Alexander (2018)].

Clearly the root causes of such multiple simultaneous events run deeper than hitherto imagined and require a different approach to be managed. The increased possibility of complex events, such as two extremes happening at the same time, and the development of cascading effects of failures affecting multiple business sectors warrants a more detailed consideration than has been evident to date.

The multiplicity of non-fatal risk, especially to "Complex and tightly coupled systems [which] are inherently vulnerable to major system accidents" [Perrow (1999)], appears to have increased proportionately together with, at least in the banking sector, "stress testing" [Xoual (2013)]. It seems perhaps that it is the "tight coupling" that is the potential "author of our pain". Perrow (1994) debated Sagan's work [Sagan (1993)] (not the astronomer) in considering "normal accident theory" in a way that laid a foundation for the more recent writings of Pescaroli and Alexander in 2015. All three authors refer to a "cascading effect" of failures or crises, which is compounded by complex related systems, in which to quote Perrow, "the initial failures cannot be contained or isolated and the system stopped; failures will cascade until a major part of the system or all of it will fail."

Most tightly coupled systems, and this includes global supply chains, are constructed as such for economic reasons and has none of the "slack" of loosely coupled systems that allows some flexibility in the face of disruption. Hence, while the world remains mostly harmless, the systems we use are at enormous risks of failure.

Let us personalize the issue and bring the matter closer to home, your home, to illustrate how tightly the world is coupled and how vulnerable it has become. Some people have invested in smart home systems so that they can turn on their home heating remotely. This uses their home wifi. The heating smart systems sometimes use old and free open-source codes, and they send the unencrypted wifi code to and from the unit. If someone can hack your heating system, they have entered your home system, which during COVID-19 you also use for your confidential work and your personal banking. A real-life incident recounted to the authors in a personal communication

[5] The term panarchy is variously attributed but on balance it seems that the playwright Ben Jonson first used the word in 1610; Ben Jonson, The Alchemist II.v.15: Ars sacra, Or chrysopoeia, or spagyrica, Or the pamphysic, or panarchic knowledge

has a similar theme. Some smart systems need a web server or cloud to work. A provider, quite remote in the supply chain, was hacked during one of the more frequent weather extremes we are experiencing. The result was no heating during the coldest week of the winter, confusion, and time lost looking for the possible gas leak before accurately identifying the problem. Mostly harmless?

3.2 Does business continuity/enterprise risk management/operational resilience work and is it worth it?

So, given the cascading Götterdämmerung imagined by Pescaroli and Alexander, Sagan, and Perrow, where "interactive and tightly coupled systems will cause a major failure, eventually," we, having turned off the heating remote, fall back on what might be termed a "distress purchase" or at best an "overhead cost" of business continuity/enterprise risk management/operational resilience.

Naturally, it is more difficult to measure the value of operational resilience, a "value protecting program", than a "value generating activity" like sales. Some companies have tried to use environmental social and corporate governance (ESG), the inheritor of CSR (corporate social responsibility), to try to tangibly measure the benefits of their "soft" efforts' contribution to the bottom line, and this might be a possible means of measurement. However, often the results of operational resilience are not reflected in some of the normal metrics that are available.

Academia has also hesitated to quantify any financial advantage in business continuity, with possibly one exception sponsored, not unsurprisingly, by the Business Continuity Institute (BCI). In reference to the earlier work of Knight and Pretty (1997), an analysis of share prices before and following incidents, it was observed by Cockram and Van Den Heuvel (2012) that "... the losers sustain approximately 15 percent drop in value, winners transform their crises into value-creating events (up to 15 percent) and emerge with enhanced reputations." But Fragouli et al. (2013) were slightly more cautious in their endorsement of planning: "it can be implied that any organization which lacks appropriate crisis management preparedness outlined through a CMP will suffer greater losses." Lindstedt (2007) noted that, "Currently as anyone working in the field is likely to say, it is not well defined by its practitioners and not well understood by its customers." Lindstedt summarized his arguments with the controversial proposition "that there is no well researched evidence that business continuity planning is beneficial." Wong (2009) suggests that despite a "myriad of information about its tactical and operational approaches ... the role of BCM at the executive level and the strategic skills of business continuity managers has not been well discussed."

These latter views contrast sharply with the marketing of operational resilience and suggest that there could be some very "elaborate and undemonstrated explanations" supporting the growing industry. Different companies may proclaim "crisis preparedness is the next competitive advantage," or could propose the resolution of all disruptions in five simple steps, all of them easily replicable with limited efforts and time. Considerable claims demand correspondingly considerable evidence and the burden of proof rests with those making the assertions. Whilst all operational resilience advocates imply benefits, nobody seems to want to quantify the return on the investment. In other words, it seems nobody has any proof at all; otherwise, they would just say it, loud and clear. In this struggle for measurement, authors such as Phelps (2018) suggested moving the discussion from "return on investment" to "value on investment" for considering the less easily quantifiable aspects of operations, such as regulatory compliance or reputation protection. However, many questions remain open about the validity of this approach.

This sounds very cynical. It is not. Business continuity/enterprise risk management/operational resilience all demand time, effort, and resources and the decision to invest further should be based on facts and not merely marketing, anecdote, audit pressure, regulation, or the rule of the very persuasive "double negative", that "we cannot be seen to not have a plan".

To demonstrate this, we would like to share details of how one major organization was able to prepare for the recent crisis, and save, or generate, in excess of U.S.$1 billion. A major multinational (with a very strong safety culture) operating in 75 countries began its pandemic planning on January 3rd, 2020 (three weeks before Wuhan was quarantined and six days before the WHO thought there could be an outbreak). Its resilience manager, who reported to the chief security officer, was a microbiologist by training. He worried about the outbreak in Wuhan and began to implement and refine their existing pandemic plan. He had the full support of the board. Their cumulative efforts are estimated to have saved or made in excess of U.S.$1 billion in revenues through being able to operate when other competitors were unable to respond as quickly in the ensuing crisis.

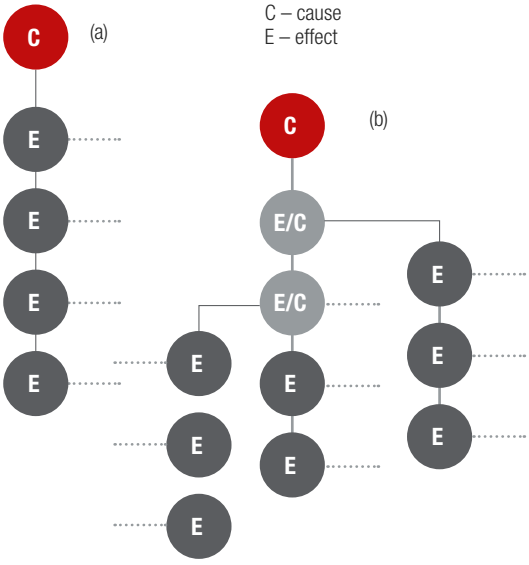
Different consulting organizations might be understandably, and rightly, apprehensive about publicizing the financial details of their clients' experiences during the crisis, but even if their marketing hyperbole is stripped away the essential argument for business continuity/enterprise risk management/ operational resilience remains sound.

3.3 How do we do it?

Now we turn to tackling the final, and frankly the most difficult question, which is how to achieve resilience.

Most advice on achieving resilience – be it "operational", "organizational", or "enterprise" – is replete with words like "dynamic", "proactive", "agility", "synergy", "intelligent", "journey", "holistic", "integrated", etc. We undertake to avoid that linguistic pitfall and to concentrate on the critical issues of cascading effects, the concurrencies between events that could arise and the requirement to stress test the organization with complex scenario exercises [Pescaroli and Alexander (2018)].

Figure 1: Linear path of events in disasters (a) and non-linear path of cascading, including amplification and subsidiary disasters (b)



Pescaroli and Alexander (2015)

3.3.1 CASCADING EVENTS

The critical issue that the slightly isolationist business continuity program does not address, and that which the enterprise risk management and operational resilience program should, is the very different nature of "cascading effects". Much of the earlier work in this area used the "toppling domino" metaphor, which naturally implies a linear sort of path. Perrow (1999) tended to this notion, deeming power grids and aircraft carrier operations as being "basically linear". They are in some respects, if one does not venture too far beyond the effects of the failure of a single entity in the whole accompanying environment or extended system. For example, "my troops on the ground were killed because they did not get the close air support from the broken aircraft carrier and so we lost the battle," is the non-linear or "cascading effect" of the failed aircraft carrier.

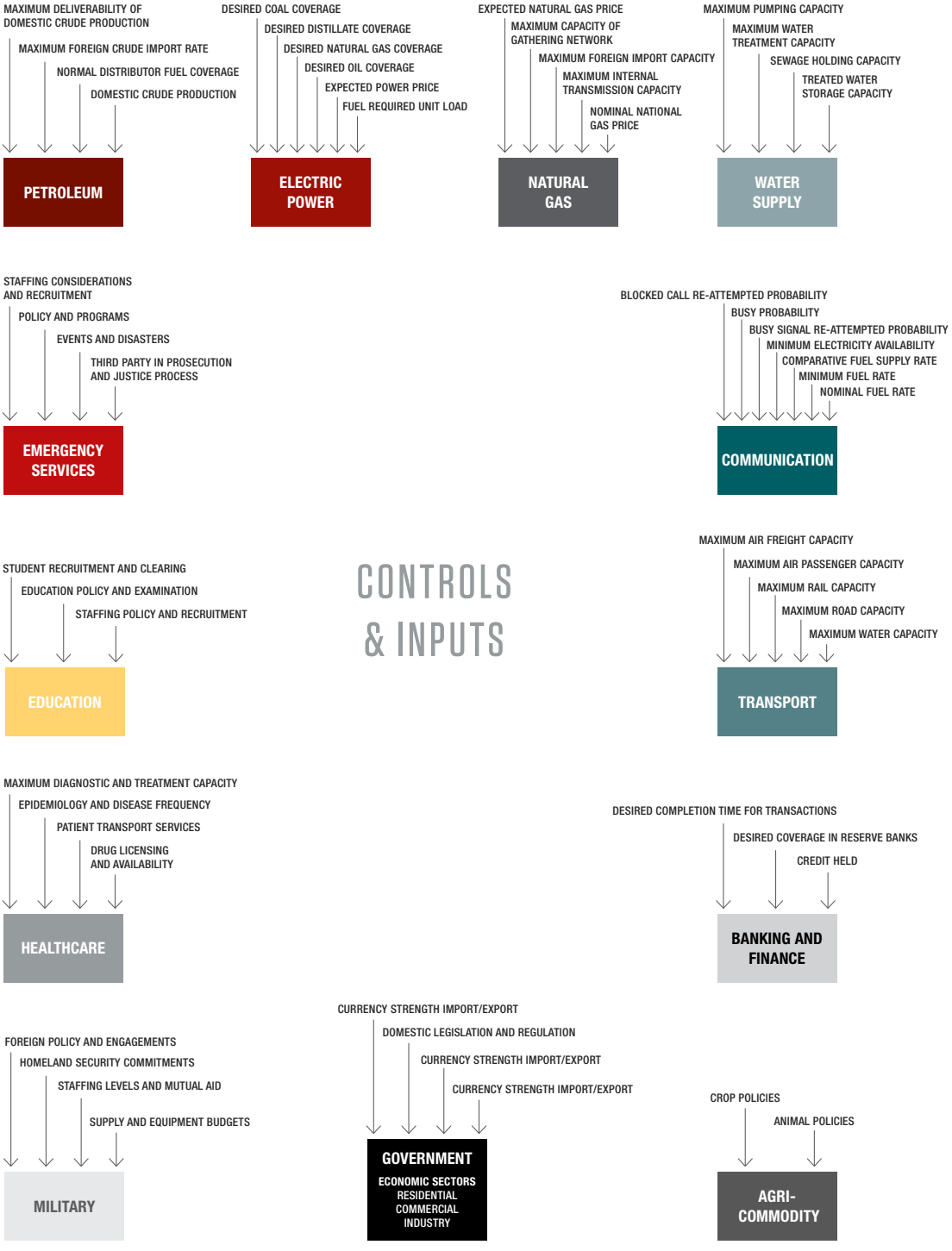
In contrast to Perrow, Pescaroli and Alexander (2015) conceptualized the path of the impact beyond the system in question and considered the effects elsewhere. Accordingly, they used the "cascade" metaphor, which better resonates in the increasingly tightly coupled world. This approach avoids conceiving disasters as a linear events and focuses the attention on what secondary emergencies could develop and become the main challenge for any emergency response (Figure 1).

While simply reframing a metaphor does not change a paradigm, it does switch perceptions from scenario planning a response to a specific linear event to reviewing and reinvigorating a focus on preparedness, which according to Pescaroli and Alexander (2016) shifts the "attention from risk scenarios based on hazard to vulnerability scenarios based on potential escalation points. That is to say, we cannot know which events can happen at the macroscopic level, but we can identify the sensitive nodes that are capable of generating secondary events at the smallest scale."

For example, the rather neat diagram in Figure 2 represents a country's infrastructure based on inputs and outputs. Start anywhere on the schematic, take out one asset or capability and plot the effects on other national infrastructure assets. Then plot the cascading effects on the others and so on. Very soon the cascading effects of the complex interactive systems make the diagram look like Figure 3.

This generates an understandable temptation to imagine that because of their regional/national/international large-scale origins, cascading disasters are low probability but high impact events, such as perhaps the Fukushima disaster. However, "they are well rooted in society's feedback loops [Alexander (2000)]. Elements such as corruption, negligence, maximization of profit and the structural weaknesses of the global socio-economic system should be seen as causes to be studied and addressed. In practical terms, the role of critical infrastructure in cascading disasters suggests that it

Figure 2: A country's infrastructure based on inputs and outputs: beginning

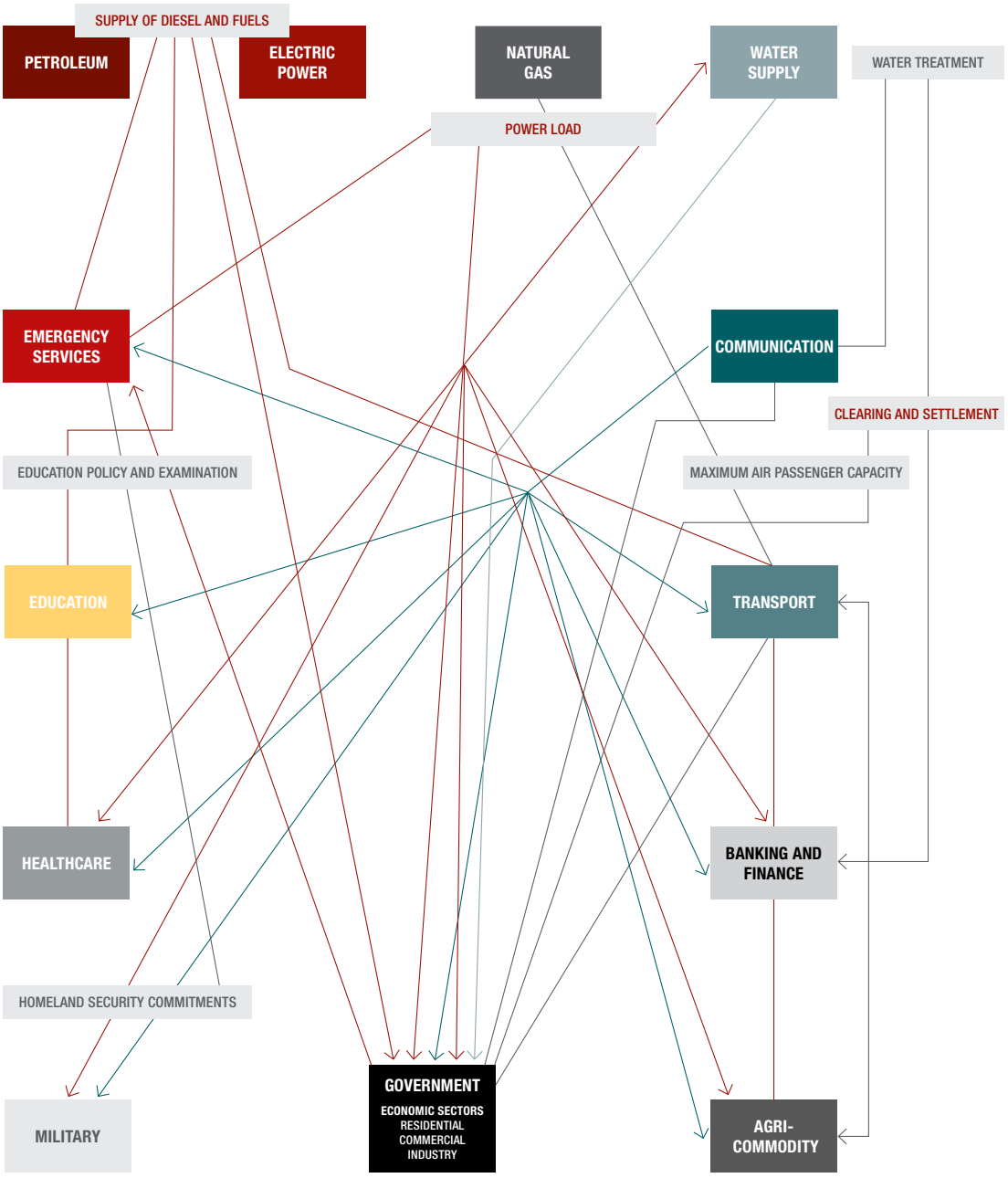


Source: Needhams 1834

is necessary to create a new culture of preparedness at the international level, for many of the scenarios involve international transboundary crises" [Pescaroli and Alexander (2016)].

This is actually what distinguishes the breadth and depth of operational resilience or enterprise risk management from the more linear and internal focus of business continuity. Operational resilience has greater focus on the flexibility of decision-making in conditions of high uncertainty, adapting the response of organizations through dynamic capabilities. To achieve this, the process of analysis requires an improved understanding of organizational structures, supply chain, and vital networks [Burnard and Bhamra (2019)].

Figure 3: A country's infrastructure based on inputs and outputs: development



To aid with understanding the image, the flows into each sector, as in Figure 2, have been removed

Source: Needhams 1834

3.3.2 STRESS TESTING

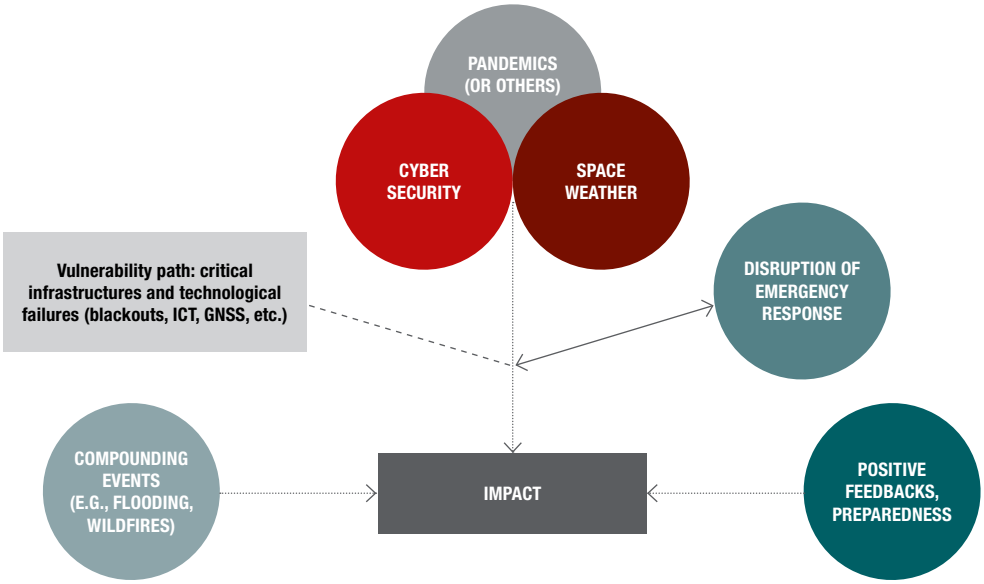
This begs the corollary question: how can organizations train themselves for such events? Many corporate "resilience" exercises have been based on the internal risks to the organization, which while worthy, tends to be business continuity-oriented and seldom reflects the cascading effects imagined in operational resilience. Almost all U.K. financial services organizations are subject to formal "stress testing" by the Financial Conduct Authority and other regulatory bodies, however the scenario topics tend to still be business-continuity oriented. Unfortunately, this is often only associated with cybersecurity, but it has much wider implications: the testing of "several but plausible scenarios" should help with understanding impact tolerances, adopting the assumption that "disruption will occur" [IA (2019)].

Before COVID-19, there was an understandable reticence by large organizations to rehearse for transnational or global events; they were deemed too unlikely, too complex, or beyond the control of the organization. In 2017, we ran two exercises, the first was based on an imaginary virus somewhat akin to COVID, and the second was a limited conflict in the South China Sea. Neither captured the imagination of the participants sufficiently for them to readily identify the cascading effects of such events; it might now. The U.K. National Risk Register is commendably full of such potential scenarios. Interestingly, Raine (2021) in a RUSI news brief[6] makes a case that half the possible issues that could be "anticipated are missing from the Register!" Nevertheless, in 2013 "severe space weather", or solar flares incubated quietly just two "grades" below pandemic. We suggested this topic to a client who was resolutely more concerned with their payment card security. This is fair enough but is indicative of the business continuity mindset rather than the operational resilience concept, where the cascading effects of a solar flare would be considerably more complex than the loss of payment card data.

The scenario itself does not have to be "complex", as the key is not in the response to the event but in the preparedness that the stress test evokes. The scenario of a solar flare is easy to author on one PowerPoint slide, the complexity of the stress test, or to be precise, the "stress", lies in the organization struggling to determine its potential degree of preparedness.

Pescaroli et al. (2018) contrasted two scenarios for increasing the resilience to complex crises and technological dependencies (Figure 4).

Figure 4: Scenarios of overwhelming disruption of operation, MORDOR



Pescaroli et al. (2018)

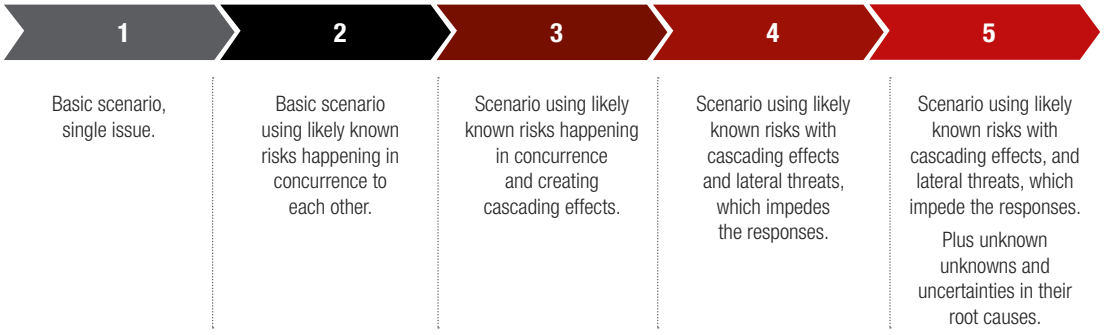
[6] https://bit.ly/3bpOGcj

In the first scenario the threat event, such as extreme space weather or cyber attacks, acts in isolation to threaten a technological network. This, in many respects reflects how the risk might be perceived in the risk register. The organizational response focuses on how to maintain the continuity of services and aims to determine which actions should have priority to minimize possible disruptions.

In the second scenario, the threat remains the same, but a cascading effect is introduced. This cascading effect denies the organization a critical ability to respond; for example, by scaling up their reactions. This inability to respond has further cascading implications that impact their operational capacity. The key issue lies in understanding the common vulnerabilities, or point of failures, that could compromise the operational capacity during scenarios that become more complex as they progress. In practical terms, the prioritization shifts to that which has not been thought through, such as the dependencies on third party providers or critical dependencies on "inviable utilities", such as satellite infrastructure like GPS/GNSS.

Such considerations are not usually identified as interdependencies on risk registers and is incredibly difficult and complex to do. Compounding the complexity of the relationships of risks, the basic awareness of such issues appears to be low. A paper in May 2020 by the Joint Centre of the European Commission considered the status of business continuity for COVID-19 within the European Reference Network for Critical Infrastructure Protection (ERNCIP) [Galbusera et al. (2021)]. The study included representatives of the banking and financial services, energy, communication, and public safety. One of the questions asked was: What is the most critical external dependency of their organization? Of some 350 multiple choices reported in the study, only five highlighted space and defense as that critical. The major problem is that the communication technology used as a "plan b" for COVID-19 depends on a global navigation satellite system (GNSS). In case of problems with GNSS, the financial sector is extremely vulnerable, from delays or interruptions in trading to marker manipulation and loss of forensic capacity [Government Office for Science (2018)].

Figure 5: Steps for the development of complexity in scenario stress-testing



The good news is that this approach to stress-testing scenarios can be easily applied within the financial services sector. First, assessing the possible disruption scenarios is part of the information gathering process for the "business impact analysis" [Storkey (2011)]. Second, "establishing impact tolerances" is very similar to assessing common vulnerabilities or point of failures, which can also be derived though the business impact analysis. What could be different is the use of creativity to go far beyond the existing planning and scenarios assumptions [Herbane (2016), Burnard and Bhamra (2019), Pescaroli and Alexander (2018)].

In summary, the scenario does not have to be complex; rather it has to uncover the common points of failure that can generate cascading effects, and therein lies the "stress" in the test. The idea is that the more closely one looks at the potential weaknesses, the more weakness may be identified in dependent areas. In other words, we begin to identify the areas that hitherto had not been identified as a being a threat.

In common with any issue, going too far too fast risks failure and the development of such scenarios can be made progressive. Basically, one can increase the variables to induce more stress as the maturity of responses increases. The five levels of magnitude proposed by Alexander (2018) can be adapted by focusing on bringing together the different forms of complex crises [Pescaroli and Alexander (2018)] and hybrid threats [Panda and Bower (2020)]. A tentative model of maturity benchmarking is offered in Figure 5.

The model begins with a scenario using the most well-known and frequent threats happening individually, such as flooding. The next step takes it to a flood caused by a storm or during a storm, which could inhibit site access. The next step introduces a cascading effect, such as the storm precipitating a power outage or damage to a communications hub, as well as a flood. A third step introduces perhaps a lateral threat that during the event a hybrid threat, such as a state inspired cyber attack or "fake news", emerges. Finally, a hypothetical "unknown-unknown" might adversely affect supporting infrastructures with resultant cascading effects.

This is hard to visualize, and the 'unknown-unknown' scenario does not need to necessarily have a detailed explanation for its emergence. At the same time, it is important that "face validity", i.e., credibility, is not compromised just to achieve a "fog of war"' scenario, nor should any scenario be used to humiliate and render the participants impotent. A brief example illustrates how a very multi-layered event can remain plausible. During the COVID-19 lockdown, climate change-induced wildfires sweep an area. This necessitates a huge breach of lockdown regulations for people in emergency shelters whose power supplies are compromised by the fire, whilst at the same time the health services fall victim to a ransomware attack. In this scenario, if the common points of failure and vulnerabilities had been imagined, anticipated, and addressed, then even though the complexity is vast, the problem would not be insoluble.

4. CONCLUSION

No responsible commentator would advocate the abandonment of corporate risk register business continuity measures and business impact analyses in favor of the sole adoption of a somewhat esoteric "sensitive node" analysis. Let us, therefore, return to the Basel Committee's definition of operational resilience, which implies that "preparedness" in advance of the events is key to its successful and meaningful implementation. "…to identify and protect itself from threats and potential failures, …to minimize their impact on the delivery of critical operations through disruption."[7]

Essentially, the argument is that historically the focus of risk management has been to determine responses to events. We are advocating that it is the degree of anticipation or preparedness that can maneuver the organization into a more resilient position in the first place and the consequent response phase will be far, far easier to implement.

This contribution to the operational resilience debate is not a panacea of prevention. Rather it is proposed, perhaps paradoxically, that because of their complex nature, cascading disasters cannot actually be prevented. But, as Pescaroli and Alexander (2016) argue: "…latent vulnerability can be understood and addressed before the trigger events occur. We need to broaden the consensus on the development of new tools and strategies."

Once again, this is in complete accord with the Basel Committee's definition of operational resilience, with the "latent vulnerabilities" being a perhaps hidden and soft underbelly of an organization's risk profile. The solution would be to adopt more systematic stress-testing, going beyond the focus on what is "thinkable". In the age of increased uncertainties, new practices for approaching scenarios are a critical tool for increasing resilience. However, a much-needed step means a shift toward assessing and testing the common vulnerabilities to the multiple threats that organizations could face. The unequivocal benefit of preparing for the "unthinkable" is being slightly more ready to deal with Rumsfeld's famous "unknown-unknowns" with more awareness about the real organizational capacity for response and recovery. In order to support this process, we proposed a preliminary benchmarking model that could bridge "blue sky" research on complexity, with practices of scenario stress testing.

In summary, this article aimed to demonstrate the value of operational resilience and offered a new putative paradigm of the value of preparedness. We hope we have achieved that. We also hope that more companies follow in the footsteps of the corporate example given in this article and establish departments for individuals who now have the job title of "Director of Strategic Anticipation".

[7] https://www.bis.org/bcbs/publ/d509.pdf

REFERENCES

Alexander, D. E., 2013, "Resilience and disaster risk reduction: an etymological journey," Natural Hazards and Earth System Sciences 13:11, 2707-2716

Alexander, D., 2018, "A magnitude scale for cascading disasters," International Journal of Disaster Risk Reduction 30, 180-185

Allen, C. R., D. G. Angeler, A. S. Garmestani, L. H. Gunderson, and C. S. Holling, 2014, "Panarchy: theory and application," Ecosystems 17:4, 578-589

Burnard, K. J., and R. Bhamra, 2019, "Challenges for organisational resilience," Continuity & Resilience Review, 1:1, 17-25

Boin, A., 2006, "Organizations in crisis: the emergence of a research paradigm," in Smith, D., and D. Elliott (eds.), Key readings in crisis management, Routledge

Cockram, D., and C. Van Den Heuvel, 2012, "Crisis management – what is it and how is it delivered," BCI Partnership.

de Puydt, P. E., 1860, Panarchy (first published in French in the Revue Trimestrielle), Bruxelles, July

Fragouli, E., A. Ioannidis, and A. Adiave Gaisie, 2013, "Crisis preparedness plans: what influences the preparedness level of an organisation and examination whether petroleum companies have crisis management plans before crises occur," International Journal of Chemical and Environmental Engineering 4:6, 363-372

Galbusera, L., M. Cardarilli, and G. Giannopoulos, 2021, "The ERNCIP survey on COVID-19: emergency & business continuity for fostering resilience in critical infrastructures," Safety Science, 105161, in press.

Government Office for Science, 2018, "Satellite-derived time and position: Blackett review," United Kingdom Government, January 30, https://bit.ly/203SozL

Herbane, B., 2016, "A business continuity perspective on organisational resilience," in IRGC, 2016, "Resource guide on resilience," EPFL International Risk Governance Center, v29-07-2016

Helbing, D., 2013, "Globally networked risks and how to respond," Nature 497:7447, 51-59

IA, 2019, "Operational resilience: business services and beyond," The Investment Association, December, https://bit.ly/3qslTbq

ISO, 2017, "ISO 22316:2017, security and resilience – organizational resilience – principles and attributes," International Organization for Standarization

ISO, 2019, "ISO 22301:2019, security and resilience – business continuity management systems – requirements," International Organization for Standarization

Linkov, I., T. Bridges, F. Creutzig, J. Decker, C. Fox-Lent, W. Kröger, J. H. Lambert, A. Levermann, B. Montreuil, J. Nathwani, R. Nyer, O. Renn, B. Scharte, A. Scheffler, M. Schreurs and T. Thiel-Clemen, 2014, "Changing the resilience paradigm," Nature Climate Change 4:6, 407-409

Lindstedt, D., 2007, "Grounding the discipline of business continuity planning: what needs to be done to take it forward?" Journal of Business Continuity & Emergency Planning l2:2, 197-205

Linnenluecke, M. K., 2017, "Resilience in business and management research: a review of influential publications and a research agenda," International Journal of Management Reviews 19:1, 4-30

NFPA, 2019, "NFPA 1600 standard on continuity, emergency, and crisis management," National Fire Protection Association

Panda, A., and A. Bower, 2020, "Cyber security and the disaster resilience framework," International Journal of Disaster Resilience in the Built Environment 11:4. 507-518

Pescaroli, G., and D. Alexander, 2015, "A definition of cascading disasters and cascading effects: going beyond the "toppling dominos" metaphor," Planet@Risk 2:3, 58-67

Pescaroli, G., and D. Alexander, 2016, "Critical infrastructure, panarchies and the vulnerability paths of cascading disasters," Nat Hazards 82, 175–192

Pescaroli, G., and D. Alexander, 2018, "Understanding compound, interconnected, interacting, and cascading risks: a holistic framework," Risk Analysis 38:11, 2245-2257

Pescaroli, G., R. T. Wicks, G. Giacomello, and D. E. Alexander, 2018, "Increasing resilience to cascading events: the M. OR. D. OR. Scenario," Safety Science 110, 131-140

Perrow, C., 1994, "The limits of safety: the enhancement of a theory of accidents," Journal of Contingencies and Crisis Management 2:4, 212-220

Perrow, C., 1999, "Organizing to reduce the vulnerabilities of complexity," Journal of Contingencies and Crisis Management 7,150-155

Phelps, R., 2018, "The true value and return on investment of business continuity," Journal of Business Continuity & Emergency Planning 11:3, 216-222

Roser, M., E. Ortiz-Ospina, and H. Ritchie, 2013, "Life expectancy," published online at OurWorldInData.org.

Sagan, C., 1974, Broca's brain: reflections on the romance of science, Ballantine Books

Sagan, S. D., 1993, The limits of safety: organisations, accidents and nuclear weapons, Princeton University Press

Smith, D., and D. Elliott, (eds.), 2006, Key readings in crisis management, Routledge

Storkey, I., 2011, "Operational risk management and business continuity planning for modern state treasuries," International Monetary Fund, Technical notes and manuals 11/05

UNISDR, 2015, "Sendai Framework for Disaster Risk Reduction 2015 – 2030," United Nations Office for Disaster Risk Reduction, https://bit.ly/3sY4ZmL

Wong, W, N. Z., 2009, "The strategic skills of business continuity managers: putting business continuity management into corporate long-term planning," Journal of Business Continuity & Emergency Planning 4:1, 62-68

Xoual, W., 2013, "The evolution of stress testing in Europe," Moody's Analytics, September, https://bit.ly/3kTWciS

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO